

AUSA: Anca I. Pop  
 Task Force Officer: Evan Zapolski  
 AO 106 (Rev. 04/10) Application for a Search Warrant

Telephone: (989) 895-5712  
 Telephone: (989) 439-5276

# UNITED STATES DISTRICT COURT

for the  
 Eastern District of Michigan

In the Matter of the Search of )  
 (Briefly describe the property to be searched )  
 or identify the person by name and address )  
 Facebook User ID: 100035389424937 and Facebook ) Case No. 19-mc-51020  
 User ID: 100005177719617 THAT IS STORED AT ) Judge: Ludington, Thomas L.  
 PREMISES CONTROLLED BY FACEBOOK, INC. ) Filed: 07-11-2019

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See ATTACHMENT A.

located in the Eastern District of Michigan, there is now concealed (identify the person or describe the property to be seized):

See ATTACHMENT B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

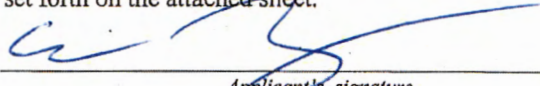
The search is related to a violation of:

Code Section	Offense Description
18, U.S.C., § 2251	Sexual exploitation of children
18, U.S.C., §§ 2252(A)(a)(2) & (a)(5)(B)	Possession of child pornography

The application is based on these facts:

See attached AFFIDAVIT.

- ☒ Continued on the attached sheet.  
☐ Delayed notice \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

  
 Applicant's signature  
 Evan T. Zapolski, TFO, FBI  
 Printed name and title

Sworn to before me and signed in my presence  
 and/or by reliable electronic means.

Date: July 11, 2019

City and state: Bay City, Michigan

  
 Judge's signature  
 PATRICIA T. MORRIS U. S. Magistrate Judge  
 Printed name and title

IN THE MATTER OF THE SEARCH OF  
INFORMATION ASSOCIATED WITH

Facebook User ID: 100035389424937 and  
Facebook User ID: 100005177719617  
THAT IS STORED AT PREMISES  
CONTROLLED BY FACEBOOK, INC.

---

AFFIDAVIT IN SUPPORT OF APPLICATION FOR A SEARCH WARRANT

1. I, Evan T. Zapolski, a Detective Trooper with the Michigan State Police, and a Task Force Officer with the Federal Bureau of Investigation, being duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

2. I am employed as a Detective Trooper (D/Tpr) with the Michigan State Police (MSP), and a Task Force Officer (TFO) with the Federal Bureau of Investigation (FBI), and have been so employed since May 2013. I have been assigned to the MSP Internet Crimes against Children Taskforce since February 2017, and have been a Task Force Officer with the FBI's Northeast Michigan Trafficking & Exploitation Crimes Taskforce since March 2019. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. I have been involved with several investigations regarding child pornography and the exploitation of children through the internet.
3. This affidavit is made in support of an application for a search warrant to search for and seize instrumentalities, fruits, and evidence of violations of Title 18,

United States Code, Sections 2251, which makes it a crime to knowingly produce child pornography, Title 18, United States Code, Sections 2252A(a)(2) and 2252A(a)(5)(B), which make it a crime to knowingly distribute, receive and possess child pornography through the use of a means and facility of interstate or foreign commerce including, but not limited to, the Internet. These items are more specifically described in Attachment B.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that Dana Nicole Taggart and Tyler Wayne Zimmerman have committed violations of 18 U.S.C. §§ 2251 and 2252A and evidence of these violations is located in and within the above listed Facebook accounts. I have reason to believe that the Facebook accounts that are the subject of the instant application will have stored information and communications that are relevant to this investigation. Thus, as outlined below, and based on my training and experience, there is probable cause to believe that evidence, fruits and/or instrumentalities of the aforementioned crimes are located in these accounts. There is also probable cause to search the information described in Attachment A for evidence of these crimes, as described in Attachment B.

### **DEFINITIONS**

5. The following definitions apply to this Affidavit and its Attachments:

- a. The term “minor,” as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.
- b. The term “sexually explicit conduct,” 18 U.S.C. § 2256(2)(A)(i-v), is defined as actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic areas of any person.
- c. The term “visual depiction,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.
- d. The term “computer,” as defined in 18 U.S.C. §1030(e)(1), means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.
- e. The term “child pornography,” as defined in 18 U.S.C. § 2256(8), means any visual depiction, including any photograph, film, video, picture, or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where

i. the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;

ii. such visual depiction is a digital image, computer image, or computer generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or

iii. such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

f. The terms “records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

g. “Internet Service Providers” (ISPs), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including

access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

6. "Internet Protocol address" (IP address), as used herein, is a code made up of numbers separated by dots that identifies a particular computer on the Internet. Every computer requires an IP address to connect to the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.
- h. "Domain names" are common, easy to remember names associated with an IP address. For example, a domain name of "www.usdoj.gov" refers to the IP address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period.
- i. "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

#### **BACKGROUND REGARDING COMPUTER, THE INTERNET, AND EMAIL**

7. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience and knowledge, I know the following:
  - a. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. It has also revolutionized the way in which child pornography collectors interact with each other. Child



pornography formerly was produced using cameras and film (either still photography or movies.) The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were definable costs involved with the production of pornographic images. To distribute these on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contact, mailings, and telephone calls. Any reimbursement would follow these same paths.

b. The development of computers has added to the methods used by child pornography collectors to interact with and sexually exploit children. Computers serve four functions in connection with child pornography. These are production, communication, distribution, and storage.

c. Child pornographers can now transfer photographs from a camera onto a computer readable format. With the advent of digital cameras, the images can now be transferred directly onto a computer. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTP) to anyone with access to a computer and

modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store hundreds of thousands of images at very high resolution.

e. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo!, Google, Inc., Facebook, Inc., among others. The online services allow a user to set up an account with a remote computing service that provides email services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by



saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner often can recover evidence suggesting whether a computer contains peer to peer software, when the computer was sharing files, and some of the files which were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

#### **TECHNICAL BACKGROUND ON FACEBOOK**

8. Facebook owns and operates a free-access social networking website of the same name that can be accessed at <http://www.facebook.com>. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.
9. Facebook asks users to provide basic contact and personal identifying information to Facebook, either during the registration process or thereafter. This information may include the user's full name, birth date, gender, contact e-mail addresses, Facebook passwords, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number to each account.

10. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with individual Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "News Feed," which highlights information about the user's "Friends," such as profile changes, upcoming events, and birthdays.
11. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create "lists" of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.
12. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post "status" updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users

can also post information about upcoming “events,” such as social occasions, by listing the event’s time, location, host, and guest list. In addition, Facebook users can “check in” to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user’s profile page also includes a “Wall,” which is a space where the user and his or her “Friends” can post messages, attachments, and links that will typically be visible to anyone who can view the user’s profile.

13. Facebook allows users to upload photos and videos, which may include any metadata such as location that the user transmitted when s/he uploaded the photo or video. It also provides users the ability to “tag” (i.e., label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Facebook’s purposes, the photos and videos associated with a user’s account will include all photos and videos uploaded by that user that have not been deleted, as well as all photos and videos uploaded by any user that have that user tagged in them.
14. Facebook users can exchange private messages on Facebook with other users. Those messages are stored by Facebook unless deleted by the user. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile. In addition, Facebook has a chat feature that allows users to send and receive instant messages through Facebook

Messenger. These chat communications are stored in the chat history for the account. Facebook also has Video and Voice Calling features, and although Facebook does not record the calls themselves, it does keep records of the date of each call.

15. If a Facebook user does not want to interact with another user on Facebook, the first user can “block” the second user from seeing his or her account.
16. Facebook has a “like” feature that allows users to give positive feedback or connect to particular pages. Facebook users can “like” Facebook posts or updates, as well as webpages or content on third-party (*i.e.*, non-Facebook) websites. Facebook users can also become “fans” of particular Facebook pages.
17. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.
18. Each Facebook account has an activity log, which is a list of the user’s posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through the account, such as “liking” a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user’s Facebook page.
19. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

20. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications (“apps”) on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that the user’s access or use of that application may appear on the user’s profile page.
21. Facebook also retains Internet Protocol (“IP”) logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Facebook profile, that user’s IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.
22. Social networking providers like Facebook typically retain additional information about their users’ accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Facebook about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider’s support services, as well as records of any actions taken by the provider or user as a result of the communications.

23. As explained herein, information stored in connection with a Facebook account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Facebook user’s IP log, stored electronic communications, and other data retained by Facebook, can indicate who has used or controlled the Facebook account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook account activity can show how and when the account was accessed or used. For example, as described herein, Facebook logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events relating to the crime under investigation. Additionally, Facebook builds geo-location into some of its services. Geo-location allows, for example, users to “tag” their location in posts and Facebook “friends” to locate each other. This geographic and timeline



information may tend to either inculcate or exculpate the Facebook account owner. Last, Facebook account activity may provide relevant insight into the Facebook account owner's state of mind as it relates to the offense under investigation. For example, information on the Facebook account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

24. Therefore, the computers of Facebook are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and other account information.

#### **FACTS SUPPORTING PROBABLE CAUSE**

25. On February 1, 2018, I was assigned cyber-tip 45209810 from the National Center for Missing and Exploited Children, hereinafter referred to as NCMEC. The cyber-tip was submitted by Tumblr and it reported that suspect username: mmhm69 had uploaded multiple files of suspected child sexually abusive material (CSAM). The cyber-tip is summarized as follows:

NCMEC TIP 45209810:

The following information was submitted to NCMEC by Tumblr:

Incident Date/Time: 01-03-2019 18:22:00 UTC

Email Address: dowork6935@gmail.com

Screen/User Name: mmhm69

Profile URL: mmhm69.tumblr.com

IP Address: 2601:408:4200:af30:5c5:807d:9738:8b34 (Other)

Suspect's last logins:

Mon, 31 Dec 2018 12:31:55 -0500 from

2601:408:4200:af30:f8eb:910e:f2b3:2a8e

Mon, 31 Dec 2018 10:01:20 -0500 from

2601:408:4200:af30:f8eb:910e:f2b3:2a8e

Sun, 30 Dec 2018 10:08:59 -0500 from 2601:408:4200:af30:f8eb:910e:f2b3:2a8e  
Wed, 12 Dec 2018 06:45:32 -0500 from 2601:408:4200:af30:b5ba:1e2a:a26:f77  
Thu, 06 Dec 2018 10:51:50 -0500 from 2601:408:4200:af30:15e0:78a0:ce2e:6

Tumblr provided five media files that were uploaded to the suspect webpage. I reviewed the files and have described two below:

File Name: 178980697910\_0\_npf\_video.mp4

This video is 47 seconds in length. It depicts a female child that looks less than 18 years old providing oral sex to a prepubescent male child, suspected to be less than 10 years old, on a bed. The male child appears to be sleeping.

File Name: 180060255965\_0\_inline\_image.gif

This .gif file depicts an erect penis being rubbed on the face of a female child.

The female has been identified as a child by NCMEC.

26. I know that IP addresses are assigned to a sole subscriber, and that the subscribing entity tracks and maintains the subscriber account info. Affiant knows that Arin.net (American Registry for Internet Numbers) can conduct a search of an IP address and return the subscribing entity name and contact information. Arin.net reported that the IP addresses 2601:408:4200:af30:f8eb:910e:f2b3:2a8e, 2601:408:4200:af30:b5ba:1e2a:a26:f77, and 2601:408:4200:af30:15e0:78a0:ce2e:6 are registered to Comcast Cable Communications, Inc.

27. I executed a search warrant to Comcast Cable Communications for the subscriber that was assigned the above stated IP addresses at the listed login dates and times. Comcast provided the following response:

Subscriber Name: Dana Taggart  
Service Address: 280 Meissner Ct, Apt. A1, Sebewaing, MI 48759  
Telephone: 989-553-0282

28. The Michigan Secretary of State reported Dana Nicole Taggart Michigan driver's license as registered to 280 Meissner Ct, Apt. 1.
29. I executed a search warrant to Google for the account dowork6935@gmail.com. Google provided account information including the name on the account; which was listed as Ty Z.
30. I searched Taggart in the Michigan State Police report writing system and observed she had multiple contacts with a William Diehl. Affiant observed Diehl was on probation reference an incident with Taggart. Michigan Department of Corrections Agent Pigott and Hulburt conducted a probation check with Diehl on May 30, 2019. Diehl stated that a Tyler Zimmerman was living with Taggart at her residence.
31. I conducted LEIN/SOS searches and located a Tyler Wayne Zimmerman with an address at 6631 Merry St, Unionville, MI. Zimmerman has a 2002 Pontiac Grand Prix with Michigan registration plate DYX8672 registered to him through the Michigan Secretary of State.
32. On May 8, 2019, D/Tpr. Green conducted mobile surveillance at the residence. He observed a female that appeared to be Taggart outside the apartment building. On May 21, 2019, D/Tpr. Green conducted surveillance at the apartment and observed the Grand Prix with registration plat DYX8672 parked outside the apartment building.

33. On June 20, 2019, a State of Michigan search warrant was executed at 280 Meissner Ct, Apt. 1, Sebewaing, Michigan. Dana Taggart and Tyler Zimmerman were interviewed on scene. Taggart and Zimmerman are in a dating relationship. Zimmerman stated he has a Samsung cell phone. A Samsung cell phone with an inserted 16 GB micro SD card was seized during the search of the apartment. Zimmerman admitted to viewing child pornography on Tumblr. Zimmerman admitted to using his phone to view child pornography.
34. While on scene, a manual review of Zimmerman's cell phone was completed. Located was a video of Taggart masturbating on her bed with her 2-year-old daughter present next to her.
35. Taggart was interviewed and admitted to making two videos of herself masturbating with her daughter in the videos. She also admitted to sending Zimmerman the videos via Facebook Messenger.
36. I completed a forensic exam on the Samsung and SD card belonging to Zimmerman. I located child pornography files on the cell phone and SD card. Some of the child pornography files depict children less than 10 years old engaging in sex acts with adults. I also located a Facebook Messenger chat between the account signed in on the device, Facebook account name: Tyler Zimmerman, User ID: 100035389424937, and the Facebook account with name: Dana Taggart, User ID: 100005177719617. The below is an excerpt from the chat that occurred on April 11, 2019:
- Dana: Glad you got to tho. Cause this I'd dealing with lol  
Tyler: Mm keep going that hot lol  
Tyler: You're my dirty mommy  
Dana: I know. She keeps rubbing me. And ugh. I just wanna come so bad.

Tyler: And I fucking love it  
Tyler: Show your pussy too  
Tyler: God mommy keep going cum for me  
Tyler: I wanna see mmm  
Tyler: God I fucking love you so much  
Dana: Save them and to take them off messenger  
Tyler: Oh I am lol

37. On the cell phone, I located five videos of Taggart masturbating that include her 2-year-old daughter. I believe Taggart sent Zimmerman the videos between the messages, "Glad you got to tho. Cause this I'd dealing with lol," and, "Mm keep going that hot lol." The five masturbation videos were saved to the Samsung cell phone on April 11, 2019, during the time the chat occurred. The videos are described below:

File Name: received\_756534401414634.mp4

This video depicts Taggart nude from the waist down, masturbating on her bed. Her daughter's foot can be seen at one point. At the end of the video, her daughter comes in to frame and she is looking at Taggart's vagina.

File Name: received\_607102239696662.mp4

This video depicts Taggart nude from the waist down, masturbating on her bed. Her daughter walks through the bedroom and Taggart continues to masturbate.

File Name: received\_567077960463613.mp4

This video depicts Taggart nude from the waist down, laying on her bed. She has a blanket over legs but her vagina is still visible. Her daughter covers Taggart's nude vagina with the blanket and then uncovers it. Taggart then starts masturbating. When Taggart starts masturbating, her daughter is laying on Taggart's right thigh staring at Taggart's vagina.

File Name: received 444704506275404.mp4

This video depicts Taggart laying on her bed with her daughter kneeling on her chest. The video begins with the focal point being Taggart but then Taggart moves the phone and her daughter is the focal point. Taggart is observed masturbating through the blanket while her daughter is on her chest.

File Name: received 2579803948913286.mp4

This video depicts Taggart nude from the waist down, masturbating on her bed. The video begins with the focal point of the video being Taggart masturbating with her hand. She moves the camera and captures her daughter in the doorway to the bedroom and continues masturbating. The camera then shifts back so her daughter cannot be seen in the doorway. Taggart continues masturbating and then again shifts the camera to capture her daughter through the bedroom doorway. The camera then shifts back so her daughter cannot be seen and she continues masturbating.

38. On June 20, 2019, I submitted preservation requests for Tyler Zimmerman and Dana Taggart's Facebook accounts.

**INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

39. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Facebook to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized



persons will review that information to locate the items described in Section II of Attachment B.

### **CONCLUSION**

40. Based on this information, I respectfully submit that there is probable cause to believe that evidence of violations of Title 18 United States Code, 2251 and 2252A will be located at in the Facebook accounts described in Attachment A.

41. Based on the forgoing, I request that the Court issue the proposed search warrant.

42. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).]

43. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

### **REQUEST TO SEAL, ORDER NON-DISCLOSURE, & KEEP ACCOUNT**

#### **ACTIVE**

44. Because the Investigation is ongoing, I requests that this Application for Search Warrant, the Search Warrant, and supporting Affidavit in this matter be sealed until such time as the Court directs otherwise.

45. Pursuant to 18 U.S.C. § 2705(b), I would request the Court order Facebook, Inc. not to notify any other person of the existence of this warrant for the next 180 days.

This request is made because I believe notification of the existence of the warrant will seriously jeopardize the ongoing investigation.

46. Because the investigation is ongoing, I would further request the Court to order Facebook, Inc. to continue to maintain the Facebook accounts associated with Tyler Zimmerman and Dana Taggart, as further detailed in Attachment A, in an open and active status.



Evan T. Zapolski  
Task Force Officer  
Federal Bureau of Investigation

Subscribed and sworn to before me and signed in my presence and/or by reliable electronic means on July 11, 2019.



Hon. Patricia T. Morris  
United States Magistrate Judge

**ATTACHMENT A**

**Property to Be Searched**

This warrant applies to information associated with the following Facebook user IDs, preserved on June 20, 2019, under Facebook case #3210701, that are stored at premises owned, maintained, controlled, or operated by Facebook Inc., a company headquartered in Menlo Park, California.

- 1) Tyler Zimmerman, Facebook User ID: 100035389424937
- 2) Dana Taggart, Facebook User ID: 100005177719617

**ATTACHMENT B**

**Particular Things to be Seized**

**I. Information to be disclosed by Facebook:**

1. To the extent that the information described in Attachment A is within the possession, custody, or control of Facebook Inc. ("Facebook"), including any messages, records, files, logs, or information that have been deleted but are still available to Facebook, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Facebook is required to disclose the following information to the government for each user ID listed in Attachment A:
  - i. All contact and personal identifying information, including full name, user identification number, birth date, gender, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.
  - ii. All activity logs for the account and all other documents showing the user's posts and other Facebook activities;
  - iii. All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them, including Exchangeable Image File ("EXIF") data and any other metadata associated with those photos and videos,
  - iv. All profile information; News Feed information; status updates; videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user

identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications;

- v. All other records of communications and messages made or received by the user, including all private messages, chat history, video calling history, and pending "Friend" requests;
- vi. All past and present lists of friends created by the account;
- vii. All records of Facebook searches performed by the account;
- viii. The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);

2. Facebook, Inc. shall disclose responsive data, if any, by sending to 6296 Dixie Hwy, Bridgeport, MI 48722 using the US Postal Service or another courier service, OR via electronic mail to ZapolskiE@Michigan.gov notwithstanding 18 U.S.C. 2252A or similar statute or code.

3. Facebook is hereby ordered to disclose the above information to the government within **14 days** of the issuance of this warrant.

**II. Information to be seized by the government**

1. All information described above in Section I that constitute fruits, evidence and

instrumentalities of violations of Title 18, United States Code, Sections 2252 and 2252A involving the users associated with the user IDs identified on Attachment A, including but not limited to information pertaining to the following matters:

- a. Any information regarding communications by the user IDs listed in Attachment A;
- b. Any person knowingly transporting, distributing, receiving, or possessing child pornography, as defined at 18 U.S.C. § 2256(8);
2. Records, including all communications, relating to who created, used, or communicated with the user IDs referenced in Attachment A, including records about their identities and whereabouts;
3. Images uploaded, downloaded, accessed, or viewed by the user IDs listed in Attachment A.

**III. By Order of the Court**

1. Pursuant to 18 U.S.C. § 2705(b), the Court orders Facebook not to notify any person of the existence of this warrant for 180 days from service of this attachment.
2. The Court further orders Facebook to continue to maintain the Facebook account associated with Harold Dubois, his aliases, and the User ID Numbers referenced in Attachment A, in an open and active status so as not to disrupt this ongoing investigation.



AUSA: Anca I. Pop

Telephone: (989) 895-5712

Task Force Officer: Evan Zapolski

Telephone: (989) 439-5276

AO 93 (Rev. 11/13) Search and Seizure Warrant

## UNITED STATES DISTRICT COURT

for the  
Eastern District of MichiganIn the Matter of the Search of )  
(Briefly describe the property to be searched )  
or identify the person by name and address) )Facebook User ID: 100035389424937 and Facebook )  
User ID: 100005177719617 THAT IS STORED AT )  
PREMISES CONTROLLED BY FACEBOOK, INC. )

Case No. 19-mc-51020

Judge: Ludington, Thomas L.

Filed: 07-11-2019

## SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Eastern District of Michigan.  
(identify the person or describe the property to be searched and give its location):

See ATTACHMENT A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

See ATTACHMENT B.

**YOU ARE COMMANDED** to execute this warrant on or before July 25, 2019 (not to exceed 14 days)☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the presiding United States Magistrate Judge on duty.  
(United States Magistrate Judge)☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)☐ for days (not to exceed 30) ☐ until, the facts justifying, the later specific date of

Date and time issued: July 11, 2019 3:42 pm

  
Judge's signature

City and state: Bay City, Michigan

Patricia T. Morris

U. S. Magistrate Judge

Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

**Return**

Case No.:

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

**Certification**

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: \_\_\_\_\_

\_\_\_\_\_  
*Executing officer's signature*\_\_\_\_\_  
*Printed name and title*

**ATTACHMENT A**

**Property to Be Searched**

This warrant applies to information associated with the following Facebook user IDs, preserved on June 20, 2019, under Facebook case #3210701, that are stored at premises owned, maintained, controlled, or operated by Facebook Inc., a company headquartered in Menlo Park, California.

- 1) Tyler Zimmerman, Facebook User ID: 100035389424937
- 2) Dana Taggart, Facebook User ID: 100005177719617

## **ATTACHMENT B**

### **Particular Things to be Seized**

#### **I. Information to be disclosed by Facebook:**

1. To the extent that the information described in Attachment A is within the possession, custody, or control of Facebook Inc. ("Facebook"), including any messages, records, files, logs, or information that have been deleted but are still available to Facebook, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Facebook is required to disclose the following information to the government for each user ID listed in Attachment A:
  - i. All contact and personal identifying information, including full name, user identification number, birth date, gender, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.
  - ii. All activity logs for the account and all other documents showing the user's posts and other Facebook activities;
  - iii. All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them, including Exchangeable Image File ("EXIF") data and any other metadata associated with those photos and videos,
  - iv. All profile information; News Feed information; status updates; videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user

identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications;

- v. All other records of communications and messages made or received by the user, including all private messages, chat history, video calling history, and pending "Friend" requests;
- vi. All past and present lists of friends created by the account;
- vii. All records of Facebook searches performed by the account;
- viii. The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);

2. Facebook, Inc. shall disclose responsive data, if any, by sending to 6296 Dixie Hwy, Bridgeport, MI 48722 using the US Postal Service or another courier service, OR via electronic mail to ZapolskiE@Michigan.gov notwithstanding 18 U.S.C. 2252A or similar statute or code.

3. Facebook is hereby ordered to disclose the above information to the government within **14 days** of the issuance of this warrant.

**II. Information to be seized by the government**

1. All information described above in Section I that constitute fruits, evidence and

instrumentalities of violations of Title 18, United States Code, Sections 2252 and 2252A involving the users associated with the user IDs identified on Attachment A, including but not limited to information pertaining to the following matters:

- a. Any information regarding communications by the user IDs listed in Attachment A;
- b. Any person knowingly transporting, distributing, receiving, or possessing child pornography, as defined at 18 U.S.C. § 2256(8);
2. Records, including all communications, relating to who created, used, or communicated with the user IDs referenced in Attachment A, including records about their identities and whereabouts;
3. Images uploaded, downloaded, accessed, or viewed by the user IDs listed in Attachment A.

**III. By Order of the Court**

1. Pursuant to 18 U.S.C. § 2705(b), the Court orders Facebook not to notify any person of the existence of this warrant for 180 days from service of this attachment.
2. The Court further orders Facebook to continue to maintain the Facebook account associated with Harold Dubois, his aliases, and the User ID Numbers referenced in Attachment A, in an open and active status so as not to disrupt this ongoing investigation.